UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ELLIOTT BROIDY and BROIDY CAPITAL MANAGEMENT, LLC,

Plaintiffs,

-against-

GLOBAL RISK ADVISORS LLC, GLOBAL RISK ADVISORS EMEA LIMITED, GRA MAVEN LLC, GRA QUANTUM LLC, GRA RESEARCH LLC, QRYPT, INC., KEVIN CHALKER, DENIS MANDICH, ANTONIO GARCIA, and COURTNEY CHALKER,

Defendants.

1:19-cv-11861-MKV

OPINION AND ORDER GRANTING IN PART DENYING IN PART MOTION TO DISMISS

MARY KAY VYSKOCIL, United States District Judge:

By this action, Plaintiff Elliott Broidy and his investment firm Broidy Capital Management ("BCM") seek to hold responsible certain actors whom he claims hacked into his email servers and distributed confidential data. Broidy claims that Defendants were hired by the nation of Qatar to perform the hacking after Broidy publicly condemned the country. In other lawsuits, Broidy has sued the nation of Qatar itself, a public relations firm and its agents, and a diplomat, all of whom are alleged to have participated in the hacking scheme. This action takes aim at the cybersecurity firm that Broidy alleges did the actual hacking of his and his company's information. Defendants have moved to dismiss Broidy's now Second Amended Complaint on both jurisdictional and substantive grounds. For the reasons that follow, Defendants' motion to dismiss is GRANTED in part and DENIED in part.

FACTUAL BACKGROUND

The Court assumes familiarity with the facts of this case and its prior decision. *Broidy v. Glob. Risk Advisors LLC*, No. 1:19-CV-11861 (MKV), 2021 WL 1225949, at *1 (S.D.N.Y. Mar. 31, 2021). The Court reviews only those facts relevant to the pending motion.[1]

The Alleged Phishing Scheme

Plaintiff Elliott Broidy is the Chief Executive Officer and Chairman of BCM. SAC ¶ 6. Outside that role, he has long been an active member of numerous political and philanthropic organizations. SAC ¶ 1. Both in these positions and on his own time, Broidy advocates against the nation of Qatar as a state-sponsor of terrorism and, in turn, a threat to U.S. national security. SAC ¶ 25. As alleged in the Second Amended Complaint, Qatar hired Defendant Global Risk Advisors ("GRA") and public relations firm Stonington Strategies LLC, among others, to silence Broidy and positively influence U.S. policy regarding relations with the country. SAC ¶¶ 37–42. Broidy alleges that Qatar specifically retained GRA, the U.S.-based cybersecurity company, to execute a hack of Broidy's personal systems and those devoted to BCM. SAC ¶¶ 39–42. Broidy alleges that prior to the hacking scheme, Qatar already had a previous relationship with GRA. Specifically, the firm allegedly had performed other hacking activities for the country, especially in relation to Qatar's efforts to host the 2022 FIFA World Cup. SAC ¶¶ 62–65.

At Qatar's direction, GRA allegedly designed a "spear phishing" campaign to hack and steal Broidy's confidential communications, which targeted Broidy's wife and his executive assistant, to ultimately gain access to BCM's servers. SAC ¶¶ 95–96. Broidy alleges that GRA and its agents maintained access to the server for approximately one month in early 2018 and, during that time, accessed attorney-client information, corporate documents, business plans, trade

[1] The facts stated herein are drawn from Plaintiff's Second Amended Complaint, ECF No. 116 ("SAC"), and are assumed to be true for the purpose of the Motion. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

secrets, and other information. SAC ¶¶ 111, 114. Defendants allegedly accessed Plaintiffs' servers while masking their IP addresses using Virtual Private Network and Virtual Private Server ("VPN") technologies from locations in Vermont, Qatar, and New York City. SAC ¶¶ 112–13.

Broidy alleges that after accessing Plaintiffs' documents, GRA and its agents disseminated them to media outlets and synchronized their efforts with the public relations team at Stonington Strategies in an effort to tarnish Broidy's reputation. SAC ¶¶ 128, 132, 144. Media outlets, including the Wall Street Journal, Huffington Post, Bloomberg, and the New York Times, then published media reports based on the hacked documents. SAC ¶ 146.

Shortly after the hacking occurred, Broidy filed a lawsuit against Qatar and its agents, including several Defendants in this action, in federal court in California. SAC ¶ 115. As alleged here, that lawsuit triggered a panic within GRA relating to evidence incriminating the company in the hacking scheme. SAC ¶ 115. In response, the CEO of GRA, Kevin Chalker ("Chalker"), allegedly instructed GRA's Chief Security Officers and a GRA Research hacker in the Reston Group, Anthony Garcia, to "wipe GRA's computers, phones, and other devices clean of any damaging evidence." SAC ¶ 115. Garcia complied with the instruction and additionally removed certain hard drives, phones, and devices from GRA's offices, brought them to a remote location, and ultimately destroyed and discarded them. SAC ¶ 115. Courtney Chalker, Kevin Chalker's brother, allegedly assisted Garcia in destroying the evidence. SAC ¶ 115.

According to the Complaint, Chalker subsequently told GRA personnel that he and GRA were responsible for the hacking operation targeting Broidy and BCM. SAC ¶ 116. Chalker also told GRA personnel that when the lawsuit was filed, he, Garcia, and Courtney Chalker had destroyed electronic devices and other materials containing evidence of the Broidy and BCM

hacking scheme in an attempt to conceal the role of GRA in the hacking. SAC ¶ 117. Chalker and GRA also allegedly directed the electronic and physical surveillance of Broidy. SAC ¶ 118.

Litigation History

This case is the latest of several litigations that Plaintiffs have brought against Qatar and its agents for the hacking and related activities. In March 2018, Broidy filed his first case in the United States District Court for the Central District of California, naming as Defendants the nation of Qatar, several Defendants in this action, and others. SAC ¶ 115; *Broidy Cap. Mgmt., LLC v. Qatar*, No. CV 18-2421-JFW(EX), 2018 WL 6074570 (C.D. Cal. 2018). The California action was ultimately dismissed on the basis of foreign sovereign immunity (as to Qatar) and personal jurisdiction (as to the other Defendants) and was affirmed by the Ninth Circuit. *Broidy Capital Mgmt, LLC v. State of Qatar*, 982 F.3d 582 (9th Cir. 2020).

Broidy then filed a case in this District against a former United Nations diplomat whom he alleges aided Qatar in the hacking and public relations conspiracy. SAC ¶ 154. That case was dismissed on the grounds of diplomatic immunity, and the dismissal was affirmed by the Second Circuit. *See Broidy Capital Mgmt. v. Benomar*, 944 F.3d 436 (2d Cir. 2019).

Finally, in early 2019, Broidy filed an action in the United States District Court for the District of Columbia against defendants related to Stonington Strategies and the firm's CEO and founder, Nicolas Muzin. SAC ¶ 37. After briefing, the court there denied a motion to dismiss raising many of the same arguments made here. *Broidy Capital Mgmt., LLC v. Muzin ("Muzin")*, No. 19-cv-0159, 2020 WL 1536350 (DLF) (D.D.C. Mar. 31, 2020). The decision was affirmed by the D.C. Circuit.[2] *See Broidy Cap. Mgmt. LLC v. Muzin*, 12 F.4th 789 (D.C. Cir. 2021). In mid-

[2] The Circuit determined that it had appellate jurisdiction because the asserted defense of conduct-based immunity for the defendants' acts allegedly taken on behalf a foreign state satisfy the requirements of the collateral order doctrine. *Broidy Cap. Mgmt. LLC v. Muzin*, 12 F.4th 789, 797 (D.C. Cir. 2021).

2022, Broidy filed a motion for reconsideration, which the district court denied. *Broidy Cap. Mgmt. LLC v. Muzin*, No. 19-CV-150, 2022 WL 1801031 (DLF), at *10 (D.D.C. 2022), *appeal dismissed*, 61 F.4th 984 (D.C. Cir. 2023).

The Pending Action

Thereafter, Plaintiff filed this action. *See* Complaint. [ECF No. 1]. An initial motion to dismiss was filed, and in response, Plaintiffs filed an Amended Complaint. *See* Amended Complaint. [ECF No. 57]. Defendants then filed a subsequent motion to dismiss the Amended Complaint, which this Court granted in whole in its March 2021 Opinion. *Broidy v. Glob. Risk Advisors LLC*, No. 1:19-CV-11861 (MKV), 2021 WL 1225949, at *1 (S.D.N.Y. 2021). In granting the motion, the Court held that although Defendants were not entitled to derivative sovereign immunity, the Amended Complaint failed to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6). *Id*. at *10. The Court found that Plaintiffs adequately alleged that Defendants had the *ability* to commit the spear phishing and hack campaign alleged in the Amended Complaint, but not that they plausibly did so. *Id*. In other words, the Amended Complaint did not plead sufficient identifiable facts that linked Defendants to the hacks in any way. *Id*. The Court allowed Plaintiffs thirty days to move for leave to file a Second Amended Complaint. *Id*.

Thereafter, Plaintiffs filed a motion for leave to file a Second Amended Complaint, declaring that they remedied the issues in the First Amended Complaint. [ECF No. 95]. Specifically, Plaintiffs claimed that they obtained and verified additional information, including a signed declaration under penalty of perjury from a former GRA employee who could connect the hacking and surveillance activity to GRA and its agents. [ECF No. 96]. Although the declarant wished to remain anonymous for alleged fear that Defendants would retaliate, Plaintiffs offered to submit, for *ex parte* and *in camera* review the former GRA employee's declaration. [ECF No. 96].

The Court granted Plaintiffs leave to file a Second Amended Complaint and denied as moot the motion to file the declaration for *ex parte, in camera* review because factual allegations in the complaint must be accepted as true at the pleadings stage. [ECF No. 114].

Plaintiffs filed their Second Amended Complaint (hereinafter "the SAC"), which is the operative complaint for purposes of this motion. The SAC asserts claims against ten Defendants. They are: Global Risk Advisors, LLC ("GRA"), a Delaware LLC with its principal place of business in New York; several of GRA's affiliated entities, including Global Risk Advisors EMEA Limited ("EMEA"), GRA Maven LLC, GRA Quantum LLC, Qrypt, Inc., GRA Research, LLC; Kevin Chalker ("Chalker"), the founder, sole member, and CEO of GRA, domiciled in New York, whom Plaintiffs allege controls all of the GRA entities; Denis Mandich, a GRA employee; Antonio Garcia, GRA's Chief Security Officer; and Courtney Chalker, Kevin Chalker's brother. SAC ¶¶ 7–22. Plaintiffs assert general personal jurisdiction in this District against Chalker and GRA based on their domiciles and specific personal jurisdiction against all other Defendants based on their business contacts in New York under New York Civil Practice Law and Rules ("CPLR") Section 302(a)(1). SAC ¶¶ 17–20.

Plaintiffs assert ten claims against various groups of Defendants. All ten claims are asserted against Defendants Chalker and GRA. Six of the claims are asserted against "All Defendants." Five of the ten claims are predicated on federal statutes, including the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* (SAC ¶¶ 174–88 [Count One]), the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) and (a)(5) (SAC ¶¶ 189–205 [Count Two]), the Defend Trade Secrets Act, 18 U.S.C. §§ 1831, 1832, 1836 (SAC ¶¶ 247–69 [Count Seven]), and the Racketeer Influenced and Corrupt Organizations Act ("RICO Act"), 18 U.S.C. §§ 1962, 1964 (SAC ¶¶ 284–341 [Count Nine – Violation of the RICO Act]; SAC ¶¶ 342–50 [Count Ten –

Conspiracy to Violate the RICO Act]). Plaintiffs also assert three California statutory claims:[3] misappropriation of trade secrets under the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426, *et seq.* (SAC ¶¶ 270–83 [Count Eight]); violation of the California Comprehensive Computer Data Access and Fraud Act, Cal. Pen. Code § 502 (SAC ¶¶ 204–19 [Count Three]); receipt and possession of stolen property in violation of Cal. Pen. Code § 496 (SAC ¶¶ 220–28 [Count Four]); and two common law claims: intrusion upon seclusion (SAC ¶¶ 229–37 [Count Five]); and civil conspiracy (AC ¶¶ 238–46 [Count Six]).

All Defendants have moved to dismiss the SAC. [ECF No. 123]. In support of their motion, Defendants filed a memorandum of law [ECF No. 124] ("Def. Br."), and a declaration of counsel [ECF No. 125]. Plaintiff opposed the motion with a memorandum of law [ECF No. 126] ("Opp."). Plaintiffs also filed a letter directing the Court's attention to the decision in *Broidy Capital Management LLC, et al. v. Nicolas D. Muzin, et al.*, Case No. 19-cv-150-DLF (D.D.C.). *See* Letter to Court from Daniel Benson dated June 2, 2022. [ECF No. 128]. Defendants then submitted a Reply Memorandum of Law. [ECF No. 129] ("Reply"). After the motion was briefed, with leave from the Court [ECF No. 144], Defendants filed a supplemental memorandum of law in support of their motion [ECF No. 145], and Plaintiffs filed a response [ECF No. 146].

LEGAL STANDARD

Defendants move to dismiss the SAC, arguing lack of personal jurisdiction, failure to state a claim pursuant to Federal Rule of Civil Procedure ("FRCP") 12(b)(6), and failure to comply with FRCP 8(a).

[3] Defendants do not dispute, for purposes of this motion, that California law governs Plaintiffs' state law claims, including the common law intrusion upon seclusion and civil conspiracy claims. Thus, the Court need not engage in a choice-of-law analysis at this time. *See Turbon Int'l, Inc. v. Hewlett-Packard Co.*, 769 F. Supp. 2d 262, 266 (S.D.N.Y. 2011) (citation omitted).

Personal Jurisdiction

To survive a Rule 12(b)(2) motion to dismiss, a plaintiff "bears the burden of demonstrating personal jurisdiction over a person or entity against whom it seeks to bring suit." *Penguin Gr. (USA) Inc. v. Am. Buddha*, 609 F.3d 30, 34 (2d Cir. 2010) (citation omitted). The plaintiff is required to make only "a prima facie showing" that jurisdiction exists. *Grand River Enters. Six Nations, Ltd. v. Pryor*, 425 F.3d 158, 165 (2d Cir. 2005) (citation omitted). At the pleading stage, such a showing "may be established solely by allegations" pleaded in good faith. *Dorchester Fin. Sec., Inc. v. Banco BRJ, S.A.*, 722 F.3d 81, 85 (2d Cir. 2013) (per curiam)). Still, jurisdiction must be alleged with "factual specificity," and conclusory statements will not suffice. *Jazini v. Nissan Motor Co.*, 148 F.3d 181, 185 (2d Cir. 1998).

Failure to State a Claim

To survive a Rule 12(b)(6) motion to dismiss, a complaint must plead "enough facts to state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

When considering a motion to dismiss a complaint under Rule 12(b)(6), the Court must "'accept[] all of the complaint's factual allegations as true and draw[] all reasonable inferences in the plaintiff's favor.' " *Siegel v. HSBC North America Holdings, Inc.*, 933 F.3d 217, 222 (2d Cir. 2019) (quoting *Giunta v. Dingman*, 893 F.3d 73, 78–79 (2d Cir. 2018)). However, the Court is " 'not bound to accept conclusory allegations or legal conclusions masquerading as factual conclusions.' " *Id*. (quoting *In re Facebook Initial Public Offering Derivative Litig.*, 797 F.3d 148, 159 (2d Cir. 2015)).

FRCP Rule 8

Rule 8(a) requires only "a short and plain statement of the claim showing that the pleader is entitled to relief," in order to "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests[.]" *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "Although [Rule] 8 does not demand that a complaint be a model of clarity or exhaustively present the facts alleged, it requires, at a minimum, that a complaint give each defendant fair notice of what the plaintiff's claim is and the ground upon which it rests." *Atuahene v. City of Hartford*, 10 F. App'x 33, 34 (2d Cir. 2001) (internal quotations omitted).

ANALYSIS

I. PERSONAL JURISDICTION OVER CERTAIN DEFENDANTS

Defendants argue that the Court lacks personal jurisdiction over: (1) the foreign Corporate Defendants—EMEA, GRA Maven, GRA Quantum, Qrypt, GRA Research; and (2) Defendant Courtney Chalker. In this Court's March 2021 Opinion, the Court expressly reserved judgment on Defendants' personal jurisdiction defenses after dismissing the First Amended Complaint in its entirety for failing to plead sufficient identifiable facts that linked Defendants to the hacks. *Broidy*, 2021 WL 1225949, at *5–8 & n.6. The Court noted that the parties' personal jurisdiction arguments "depend[ed] in large part on whether Plaintiffs' RICO claims survive." *Id*. Defendants now incorporate their previous personal jurisdiction arguments by reference into their briefings on the pending motion. Def. Br. at 25 (citing Defendants' Motion to Dismiss the First Amended Complaint, Sections I and II [ECF No. 73]). Plaintiffs do not readdress Defendants' previous personal jurisdiction arguments in their briefings on this motion.

The SAC claims personal jurisdiction over these Defendants pursuant to the RICO Act's Jurisdictional Provision (18 U.S.C. § 1965) and New York Civil Practice Law and Rules ("CPLR")

Section 302(a)(1). SAC ¶¶ 19–20. As discussed in detail below, *see infra* Section III(d), the Court dismisses Plaintiffs' RICO claims (Claims XI and X), therefore precluding a personal jurisdiction basis under Section 1965 of the RICO Act. Accordingly, the Court only analyzes whether it has personal jurisdiction over these Defendants pursuant to CPLR Section 302(a)(1).

First, the Court must determine whether the law of the forum state, here, New York's long-arm statute, CPLR Section 302(a), would subject these Defendants to personal jurisdiction. *See Int'l Shoe Co. v. State of Wash., Off. of Unemployment Comp. & Placement*, 326 U.S. 310, 319 (1945); *Bank Brussels Lambert v. Fiddler Gonzalez & Rodriguez*, 305 F.3d 120, 124 (2d Cir. 2002). If New York law would permit the exercise of jurisdiction over the Defendants, the Court must also evaluate whether the exercise of jurisdiction would comport with due process. *See Friedman v. Bloomberg L.P.*, 884 F.3d 83, 90 (2d Cir. 2017).

Section 302(a)(1) of New York's long-arm statute authorizes the exercise of personal jurisdiction over anyone who, "in person or through an agent . . . transacts any business within the state or contracts anywhere to supply goods or services in the state." A party "transacts business" within New York when it "purposefully avails itself of the privilege of conducting activities within New York." *Ehrenfeld v. Bin Mahfouz*, 9 N.Y.3d 501, 508, 881 N.E.2d 830 (2007) (cleaned up). To establish personal jurisdiction under Section 302(a)(1), the asserted claim must "arise from" the defendant's business activities within New York. A claim "arises from" a transaction "when there is some articulable nexus between the business transacted and the claim sued upon, or when there is a substantial relationship between the transaction and the claim asserted." *Sole Resort, S.A. de C.V. v. Allure Resorts Mgmt.*, LLC, 450 F.3d 100, 103 (2d Cir. 2006) (internal quotations omitted); *McGowan v. Smith*, 52 N.Y.2d 268, 273, 437 N.Y.S.2d 643, 419 N.E.2d 321 (1981); *Kreutter v. McFadden Oil Corp.*, 71 N.Y.2d 460, 467, 527 N.Y.S.2d 195, 522 N.E.2d 40 (1988).

A. The SAC Fails to Allege Personal Jurisdiction Over Courtney Chalker.

Plaintiffs fail to allege that the Court has personal jurisdiction over Courtney Chalker. First, Plaintiffs make no allegations regarding Courtney Chalker's business or residency. With respect to Section 302(a)(1), Plaintiffs make no allegations that Courtney Chalker "transact[ed] business" of any kind in New York. In fact, the SAC fails to allege any act whatsoever that Courtney Chalker may have taken in New York, regardless of whether that conduct relates to business transactions giving rise to the claims in this case. To be sure, the SAC specifically alleges that he assisted Defendant Garcia in destroying electronic devices and other materials related to the hacking scheme. SAC ¶ 117. However, the SAC provides no detail to clarify where that conduct took place. Nor can it be said that the acts taken by Kevin Chalker or GRA in New York are attributable to Courtney Chalker under an agency theory because neither Kevin Chalker nor GRA is *Courtney Chalker's* agent. *See* NY CPLR § 302(a)(1) (conferring jurisdiction for actions committed "in person or *through* an agent"). To the contrary, the Plaintiffs specifically allege that *Courtney Chalker acted as an agent* of Kevin Chalker and GRA—not the other way around. SAC ¶¶ 20, 59. As such, the Court finds that Plaintiffs fail to allege that this Court has personal jurisdiction over Courtney Chalker under CPLR Section 302(a)(1) and grant Defendants' motion to dismiss all claims against him.[4]

[4] The fact that the Court ultimately concludes Plaintiffs adequately pleaded Courtney Chalker and Chalker are co-conspirators is irrelevant for purposes of personal jurisdiction under CPLR Section 302. "To warrant the inference that a defendant was a member of the conspiracy [*for jurisdictional purposes*], Plaintiffs must show that "(a) the defendant had an awareness of the effects in New York of its activity; (b) the activity of the co-conspirators in New York was to the benefit of the out-of-state conspirators; and (c) the co-conspirators acting in New York acted at the direction or under the control or at the request of or on behalf of the out-of-state defendant." *Maersk, Inc. v. Neewra, Inc.*, 554 F. Supp. 2d 424, 442–43 (S.D.N.Y. 2008) (citing *In re Terrorist Attacks of September 11, 2001*, 349 F. Supp. 2d 765, 805 (S.D.N.Y.2005)). Plaintiffs plead no factual allegations that Kevin Chalker and GRA were acting "at the direction or under the control or at the request of or on behalf of [Courtney Chalker]" or "to the benefit of" him. The SAC pleads the opposite. *Courtney* Chalker acted at the direction of Kevin Chalker and GRA—not the other way around. SAC ¶¶ 20, 59.

B. The SAC Fails to Allege Personal Jurisdiction Over the Foreign Corporate Defendants.

With respect to the foreign Corporate Defendants, the SAC does not plead any facts related to principal places of business or states of incorporation for these Defendants. While the SAC expressly pleads that Chalker is a "*sole member* of GRA, which he operates and controls," SAC ¶ 9, the SAC is notably silent as to the members and owners of each foreign Corporate Defendant. Several of the foreign Corporate Defendants are LLCs. The owners of an LLC are called members—a point of which Plaintiffs are clearly aware given their pleading GRA's membership. *See* SAC ¶ 9. The SAC also does not allege that these foreign Corporate Defendants "transact[] any business," "contract[] anywhere," or "regularly do[] or solicit[] business" in New York. *See* NY CPLR § 302(a)(1). Nor does the SAC allege any act whatsoever that the foreign Corporate Defendants purportedly took in New York, much less that such conduct relates to business transactions giving rise to the claims at issue.

Instead, the SAC appears to rely solely on the allegations that "Chalker [a New York domiciliary] owns and/or controls [these] affiliated entities," *see* SAC ¶ 9, and "Defendants GRA [a New York-based corporation], GRA Maven, GRA Quantum, GRA EMEA, Qrypt, and GRA Research . . . are co-conspirator entities . . . [that] operate as separate but intertwined departments of a single company whose finances are thoroughly comingled," SAC ¶ 292. But these vague allegations do not give rise to personal jurisdiction under Section 302(a)(1).[5] In the absence of specific or general personal jurisdiction, the Court grants the Defendants' motion to dismiss all claims against the foreign Corporate Defendants.

[5] The Court also notes that the acts taken by Chalker and GRA in New York cannot be attributed to the foreign Corporate Defendants under agency theory for the same reason they cannot be attributed to Courtney Chalker under an agency theory. Plaintiffs specifically allege that the foreign Corporate Entities acted under the control of Chalker and GRA—not the other way around. SAC ¶ 9. Thus, Chalker and GRA, who allegedly did act in New York, are *not* agents of the foreign Corporate Defendants, that have no New York ties.

II. SUFFICIENCY OF ALLEGATIONS UNDER RULE 8(a).

Defendants further argue that the SAC violates the notice pleading requirements of Rule 8(a) in two ways: (1) the factual allegations from an anonymous declarant do not adequately specify that the declarant was in a position to know such facts; and (2) the SAC groups the Defendants in a way that fails to give each Defendant fair notice of the claims against it.

A. The Factual Allegations from the Anonymous Declarant Are Accepted as True for Purposes of This Motion.

Since its last amendment, the primary changes in the SAC stem from an anonymous declarant—a former GRA employee whom Plaintiffs reportedly have interviewed in connection with this action. Defendants argue, however, that, in violation of Rule 8(a), Plaintiffs provide no factual basis in the SAC to plausibly infer that the declarant was in a position to know of Defendants' alleged involvement in the hacking.

First, the only cases that Defendants cite as support are securities fraud cases analyzed under "the heightened pleading requirements of Federal Rule of Civil Procedure 9(b)." *See In re Weight Watchers Int'l Inc. Sec. Litig.*, 504 F. Supp. 3d 224, 242 (S.D.N.Y. 2020). Defendants cite no authority applying a heightened pleading standard to declarations in cases where the relevant standard, as here, is Rule 8. Under the applicable Rule 8(a) pleading standard, the allegations based on information received from the declarant—which are presumed true for purposes of this motion, *see Siegel*, 933 F.3d at 222 (2d Cir. 2019)—are sufficient. Indeed, after denying as moot Plaintiffs' invitation to review *ex parte* and *in camera* the declaration in its unredacted form, the Court held that "the factual allegations contained in the Proposed Second Amended Complaint" are accepted "as true at this stage[.]" [ECF 114, at 4]. *See Siegel*, 933 F.3d at 222.

B. The SAC is Adequately Specific as to Each Defendant.

In this action, Plaintiffs assert six of their claims against "All Defendants." Defendants argue that Plaintiffs have violated Rule 8(a) by failing to give each Defendant fair notice of the claims against it. Specifically, Defendants argue that Plaintiffs fail to specify the wrongful conduct attributable to each Defendant and instead lump their causes of action together against "All Defendants."

The Second Circuit's precedent does not require that a "complaint separate out claims against individual defendants," *Wynder v. McMahon*, 360 F.3d 73, 80 (2d Cir. 2004), or "prohibit[] collectively referring to multiple defendants where the complaint alerts defendants that identical claims are asserted against each defendant." *Consumer Fin. Prot. Bureau v. RD Legal Funding, LLC*, 332 F. Supp. 3d 729, 771 (S.D.N.Y. 2018) (citation omitted). At a minimum, "[Rule 8] requires that a complaint give each defendant fair notice of what the plaintiff's claim is and the ground upon which it rests." *Atuahene*, 10 F. App'x at 34 (internal quotations omitted). In other words, "[w]here a complaint names multiple defendants, that complaint must provide a plausible factual basis to distinguish the conduct of each of the defendants." *Ochre LLC v. Rockwell Architecture Plan. & Design, P.C.*, 2012 WL 6082387, at *6–7 (S.D.N.Y. 2012), *aff'd*, 530 F. App'x 19 (2d Cir. 2013) (emphasis added).

Plaintiffs have added several factual allegations to the SAC that describe the specific actions taken by Individual Defendants Denis Mandich, Antonio Garcia, and Chalker. *See e.g.*, SAC ¶ 57 ("Mandich's job duties included designing the "special projects" at the direction of Chalker"); SAC ¶ 58 ("Garcia . . . worked as GRA's chief information officer and under Chalker's direct control . . . assisted Chalker by destroying evidence, including electronic devices, of the Broidy hacking after Broidy initiated litigation"); SAC ¶ 60 ("Mandich was the mastermind behind

the Global Leaks operation, overseeing the execution of every phase of the operation."); SAC ¶ 60 ("On information and belief, John Sabin and Defendants Garcia and Kevin Chalker also worked with Mandich in carrying out the Global Leaks campaign."); SAC ¶ 292 ("Defendants Mandich and Garcia are key operatives who at times shared oversight and management responsibility with Chalker.").

The Court acknowledges that the SAC is not entirely specific insofar as the Claims Section frequently attributes certain conduct or actions generally to "All Defendants." However, Rule 8 "does not demand that a complaint be a model of clarity or exhaustively present the facts alleged." *Atuahene*, 10 F. App'x at 34. In reaching a conclusion, the Court also considers the fact that the Individual Defendants are expressly alleged to work as co-conspirators and under the control and direction of Chalker. *See e.g.*, SAC ¶¶ 239, 245, 291. Therefore, it is not unusual that many of the allegations pertain to more than one Defendant. In fact, a complaint may "allege[] joint activity" by various defendants without having to "elaborate extensively on the details with regard to each defendant." *Vantone Group Ltd. Liability Co. v. Yangpu NGT Indus. Co., Ltd.*, 2015 WL 4040882, at *4 (S.D.N.Y. July 2, 2015); *see also In re Morgan Stanley ERISA Litig.*, 696 F. Supp. 2d 345, 365 (S.D.N.Y. 2009) ("Rule 8 does not require Plaintiffs to identify each Defendant by name when the Complaint makes an allegation that applies equally to all"); *In re Polaroid ERISA Litig.*, 362 F. Supp. 2d 461, 471 (S.D.N.Y. 2005) ("The fact that most of Plaintiffs' claims apply to all Defendants and that the factual allegations refer to them collectively does not render the Complaint violative of Rule 8").

As such, the Court finds that Plaintiffs meet the minimum pleading requirements under Rule 8(a) by providing the Individual Defendants with "a plausible factual basis to distinguish the conduct of each of the defendant[]." *Ochre*, 2012 WL 6082387, at *6–7.

III. FAILURE TO STATE A CLAIM UNDER RULE 12(B)(6).

Defendants next argue that Plaintiffs' causes of action must be dismissed because they each fail to state a claim under Rule 12(b)(6).

A. Stored Communications Act

First, Plaintiffs assert a claim in Count I against GRA and Chalker, as primary actors, for violation of the Stored Communications Act, 18 U.S.C. § 2701, *et seq*. ("SCA"). SAC ¶¶ 174–88 (Claim I). The SCA provides a private cause of action against a defendant who "intentionally accesses without authorization a facility through which an electronic communication service is provided." 18 U.S.C. §§ 2701(a)(1), 2707(a). Defendants argue that Plaintiffs allege hacking of personal computers and BCM's computer systems, which they contend are not cognizable "facilities" under the SCA.

While the SCA does not include a definition of "facility," it does define "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (incorporated by reference in 18 U.S.C. § 2711(1)). Although the Second Circuit has not yet ruled on the issue, courts in this district have consistently declined to treat personal computers as "facilities" for SCA purposes. *See, e.g.*, *Williams v. Rosenblatt Securities Inc.*, 136 F. Supp. 3d 593, 607 (S.D.N.Y. 2015) (dismissing SCA claim because communications downloaded to a user's computer terminal are neither stored on a temporary basis "incident to [their] electronic transmission" nor stored "by an electronic communication service); *Cohen v. Casper Sleep Inc.*, No. 17-CV-9325, 2018 WL 3392877, at *5 (S.D.N.Y. 2018) ("Judges in this District routinely hold that communications stored on personal devices are not held in electronic storage"); *Obeid on behalf of Gemini Real Estate Advisors LLC v. La Mack*, No. 14-CV-6498, 2017 WL 1215753, at *9 (S.D.N.Y. 2017) (affirming

that stored communications subject to the SCA are emails stored on an electronic communication service provider's systems, not those stored on personal computers).[6]

When passing the SCA, Congress was motivated by "a specific congressional intent to deal with the particular problem of private communications *in network service providers' possession*." *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 147 (3d Cir. 2015) (emphasis added). The statute naturally applies to telephone companies, internet or e-mail service providers, and bulletin board services, but not personal devices that simply *make use of* rather than *provide* electronic communication services. *See* S. REP. No. 99–541, at 36, reprinted in 1986 U.S.C.C.A.N. 3555, 3590; *see also Garcia*, 702 F.3d at 792; *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004). As a result, the personal computers of Broidy's wife and secretary, as well as BCM's private computer systems, do not qualify as "facilities" for SCA purposes.

Defendants further argue that Plaintiffs' claim that Defendants also accessed "Google's servers," *see* SAC ¶ 179—which unquestionably constitute a "facility" under the SCA—fails as a vague and conclusory allegation. However, Plaintiffs' claim that Defendants accessed "Google's servers" finds factual basis in various other allegations that the spear phishing "emails were disguised to appear as though they were Google security alerts, and they asked [Plaintiffs] to enter their Gmail login credentials." SAC ¶ 100. Moreover, the Complaint alleges that Defendants ultimately did access and modify the Gmail accounts of Broidy's wife and executive assistant, which allowed Defendants to read, send, delete, and manage their Gmail emails and eventually obtain their login-credentials for the BCM server. *See e.g.*, SAC ¶¶ 102–03.

[6] Most courts outside of the Second Circuit have reached the same conclusion. *See e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 277 (3d Cir. 2016) (finding that "personal computing devices were not protected 'facilities' under the statute"); *Garcia v. City of Laredo, Texas*, 702 F.3d 788, 792 (5th Cir. 2012) (concluding that the SCA "does not apply to data stored in a personal cell phone"); *United States v. Steiger*, 318 F.3d 1039, 1048 (11th Cir. 2003) (finding that the SCA does not apply to the act of hacking into a personal computer to download information stored on the hard drive).

Accordingly, the Court finds that Plaintiffs adequately allege that Defendants hacked Google's servers, which are cognizable "facilities" under the SCA. As such, the Court denies Defendants' motion to dismiss the SCA claim (Count I) against Kevin Chalker and GRA.

B. Computer Fraud and Abuse Act and its analog California Comprehensive Computer Data Access & Fraud Act

Plaintiffs assert a claim under the Computer Fraud and Abuse Act ("CFAA") (Count II) against all Defendants and a claim under its state analog, the California Comprehensive Computer Data Access and Fraud Act ("CDAFA") (Count III) against Chalker and GRA. SAC ¶¶ 189–219 (Claims II, III). The CFAA penalizes one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2). A "protected computer" includes one that "is used in or affect[s] interstate or foreign commerce or communication." *Id*. § 1030(e)(2). "Any person who suffers damage or loss by reason of a violation of [the Computer Fraud and Abuse Act] may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." *Id*. § 1030(g).

Defendants argue that Plaintiffs' claims under the CFAA and CDAFA, fail because Plaintiffs do not adequately plead the required damages under either statute. The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Further, the statute defines "loss" as "a reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Lastly, a plaintiff alleging damages for a CFAA claim must

plead only that the aggregate value of the loss be in excess of $5,000, *see* 18 U.S.C. § 1030(c)(4)(a)(1)(I).

While "physical damage to a computer is not necessary to allege damage or loss," damages and losses are limited to "computer-related constructs." *Schatzki v. Weiser Cap. Mgmt., LLC*, No. 10 CIV. 4685, 2012 WL 2568973, at *2 (S.D.N.Y. 2012) (citing *Bose v. Interclick, Inc.*, 10–9183(DAB), 2011 WL 4343517, at *3 (S.D.N.Y. 2011) and *Garland–Sash v. Lewis*, No. 05–6827(WHP), 2012 WL 6188712, at *2 (S.D.N.Y. 2011)). Courts in this district have recognized damages and losses to "computers, systems or data that could require economic remedy" as well as economic losses born "in securing or remedying their systems." *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 524–25 (S.D.N.Y. 2001); *see also Schatzki*, 2012 WL 2568973, at *2. For example, a "loss" may include the costs of seeking to "identify evidence of the breach, assess any damage it may have caused, and determine whether any remedial measures were needed to rescue the network." *Univ. Sports Pub. Co v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 383 (S.D.N.Y. 2010); *Schatzki*, 2012 WL 2568973, at *2.

Here, the SAC alleges that GRA and Chalker directly caused Plaintiffs to "incur[] substantial losses and damage," including but not limited to "losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of forensic investigators, data security experts, and attorneys." SAC ¶ 203. The SAC also alleges losses associated with remedial measures, including "the replacement costs for personal and business computers and cell phones," and "consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems." SAC ¶ 203. Finally, the SAC alleges that the total amount of losses "far exceeds $75,000" and that "out-of-pocket costs paid to outside

consultants to conduct a damage assessment for remedial measures was alone in the hundreds of thousands of dollars." SAC ¶ 204.

As such, Plaintiffs adequately allege "computer-related" losses under the CFAA and its analog CDAFA.[7] The Court denies Defendants' motion to dismiss Count II against all remaining Defendants and Count III against Chalker and GRA.

C. Defend Trade Secrets Act and Its Analog California Uniform Trade Secrets Act

Plaintiffs also assert a claim under the Defend Trade Secrets Act, 18 U.S.C. §§ 1831, 1832, 1836 ("DTSA") (Count VII) against all Defendants and a claim under its state analog, the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 ("CUTSA") (Count VIII) against Chalker and GRA. SAC ¶¶ 247–83 (Counts VII, VIII). Defendants allege that Plaintiffs' DTSA and CUTSA claims fail because (1) Plaintiffs do not adequately plead that they possessed any trade secrets (2) nor do Plaintiffs plausibly allege any Defendant misappropriated any trade secrets. The Court need not reach Defendants' second argument, because Plaintiffs' DTSFA claim fails under the first prong of the DTSA test.[8]

[7] Both parties concede that "incur[ing] costs as a result of investigating and conducting a damage assessment" tied to a hack are cognizable under the CDAFA. *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 964 (N.D. Cal. 2014). Unlike the CFAA, the CDAFA does not impose a $5,000 loss minimum—any amount of damage or loss caused by the defendant's CDAFA violation is enough to sustain the plaintiff's claims. *Id*. Thus, courts have found that a plaintiff's alleged damage or loss may be sufficient to support a CDAFA claim even where it is not enough to support a claim under the CFAA. *Id*. (citing *Mintz v. Mark Bartelstein & Associates Inc.*, 906 F. Supp. 2d 1017, 1029 (C.D. Cal. 2012); *Capitol Audio Access, Inc. v. Umemoto*, 980 F. Supp. 2d 1154, 1157–60 (E.D. Cal. 2013)). Accordingly, the Court finds that Plaintiffs adequately allege losses under CDAFA for the same reasoning it finds Plaintiffs adequately allege losses under CFAA.

[8] "Courts have held that the DTSA and the CUTSA share the same pleading requirements for the identification of trade secrets." *Alta Devices, Inc. v. LG Elecs., Inc.*, 343 F. Supp. 3d 868, 880–81 (N.D. Cal. 2018); *see also InteliClear, LLC v. ETC Glob. Holdings, Inc.*, 978 F.3d 653, 657 (9th Cir. 2020) ("Courts have analyzed these claims together because the elements are substantially similar."); *Genasys Inc. v. Vector Acoustics, LLC*, 638 F. Supp. 3d 1135, 1150 (S.D. Cal. 2022). As such, the Court finds that Plaintiffs fail to state a claim under CUTSA for the same reasoning it finds Plaintiffs fail to state a claim under DTSA.

The DTSA permits plaintiffs to bring a private cause of action if they "own[] a trade secret that is misappropriated." 18 U.S.C. § 1836(b)(1). Under the DTSA, a "trade secret" includes "all forms and types of financial, business, scientific, technical, economic, or engineering information" so long as (1) the owner "has taken reasonable measures to keep such information secret" ***and*** (2) "*the information derives independent economic value, actual or potential, from" its secrecy*. 18 U.S.C. § 1839(3) (emphasis added).

The Second Circuit has not "expressly required trade secrets to be identified with any particular degree of specificity." *Broker Genius, Inc. v. Zalta*, 280 F. Supp. 3d 495, 514 (S.D.N.Y. 2017) (citing, *inter alia*, *Heyman v. AR. Winarick, Inc.*, 325 F.2d 584, 588–90 (2d Cir. 1963)). However, "to survive a motion to dismiss, a party alleging that it owns a trade secret must put forth *specific allegations* as to the information owned *and its value*." *Elsevier Inc. v. Doctor Evidence*, LLC, No. 17cv5540, 2018 WL 557906, at *4 (S.D.N.Y. Jan. 23, 2018) (emphasis added). While it is "not necessary to disclose every detail of an alleged trade secret in a complaint[,]" a plaintiff must allege more than "conclusory statements that simply *restate the elements of a trade secret*." *Democratic Nat'l Comm. v. Russian Fed'n*, 392 F. Supp. 3d 410, 448 (S.D.N.Y. 2019) (citing *Elsevier*, 2018 WL 557906, at *4); *Lawrence v. NYC Med. Practice*, P.C., No. 18-CV-8649, 2019 WL 4194576, at *4 (S.D.N.Y. Sept. 3, 2019) (citation omitted).

Here, Plaintiffs allege in a conclusory, boilerplate manner that their trade secrets "derive independent value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use." *See* SAC ¶ 257. The allegation improperly recites the exact language found in Section 1839. *See* 18 U.S. Code § 1839(3)(B) ("the term 'trade secret' means . . . the information derives independent economic value . . . from not being generally known to, and not being readily ascertainable . . . by, another person who can

obtain economic value from the disclosure or use"). This is precisely the kind of generic allegation that courts hold insufficient. *See Democratic Nat'l Comm*, 392 F. Supp. 3d at 448; *see also Lawrence*, 2019 WL 4194576, at *5 (dismissing DTSA claim where defendants "fail to include any allegations supporting [*inter alia*] . . . the information's value, the extent to which it is known by those within and outside of the business, . . . and the ease with which the information could be acquired or developed by outsiders").

Plaintiffs also briefly allege that their "trade secrets have significant value, resulting from significant investment of time and resources." *See* SAC ¶ 258. However, this allegation similarly fails to carry Plaintiffs' burden to establish that the information at issue is a trade secret. *24 Seven, LLC v. Martinez*, No. 19-CV-7320 (VSB), 2021 WL 276654, at *9 (S.D.N.Y. 2021) (rejecting plaintiff's DTSA claim where it alleged in the absence of any other facts "that its time and resources spent compiling [] data demonstrate that [plaintiff] derives economic value from the information in question"). Plaintiffs here make no other allegations as to the economic value of their purported trade secrets vis-à-vis its competitors. *See e.g.*, *24 Seven*, 2021 WL 276654, at *9 (rejecting plaintiff's argument that information derived independent economic value because the complaint did not allege how or why it gave plaintiff "an economic leg up over competitors who do not know or use it"); *see also Inv. Sci., LLC v. Oath Holdings Inc.*, No. 20 CIV. 8159 (GBD), 2021 WL 3541152, at *4 (S.D.N.Y. 2021) (same).

Ultimately, Plaintiffs allege nothing more than a formulaic recitation of an element of a DTSA claim, which clearly fails under *Twombly*. 550 U.S. at 570 (holding a complaint must plead "enough *facts* to state a claim to relief that is plausible on its face"). As such, Plaintiffs' DTSA claim (Count VII) and their CUTSA claim (Count VIII) are dismissed in their entirety.

D. RICO Act and Conspiracy to Violate RICO Act

Plaintiffs assert two claims under the Racketeer Influenced and Corrupt Organizations Act ("RICO Act"). First, Plaintiffs claim a violation of the RICO Act pursuant to 18 U.S.C. §§ 1962(c) and 1964 against all Defendants (Count IX). SAC ¶¶ 284–341. Second, Plaintiffs allege a claim for Conspiracy to Violate the RICO Act against all Defendants (Count X). SAC ¶¶ 342–50. Defendants argue that Plaintiffs are collaterally estopped from asserting these RICO claims against the Defendants in this case, who were the alleged co-conspirators of the defendants in *Broidy Capital Mgmt., LLC v. Muzin ("Muzin")*, No. 19-cv-0159 (DLF), 2020 WL 1536350 (D.D.C. Mar. 31, 2020), since the RICO claims in *Muzin* were dismissed for failure to state a claim.

Under the doctrine of defensive collateral estoppel, also called issue preclusion, a plaintiff is prevented from "relitigating in a subsequent action an issue of fact or law that was fully and fairly litigated in a prior proceeding." *Austin v. Downs, Rachlin & Martin Burlington St. Johnsbury*, 270 F. App'x 52, 53 (2d Cir. 2008). Federal law applies to determine the preclusive effect of a prior federal judgment. *Id*. Under federal law, collateral estoppel applies when: "(1) the identical issue was raised in a previous proceeding; (2) the issue was actually litigated and decided in the previous proceeding; (3) the party had a full and fair opportunity to litigate the issue; and (4) the resolution of the issue was necessary to support a valid and final judgment on the merits." *Id*. (quoting *Interoceanica Corp. v. Sound Pilots, Inc.*, 107 F.3d 86, 90 (2d Cir.1997)).

There are two types of defensive collateral estoppel—mutual and non-mutual. *Parklane Hosiery Co. v. Shore*, 439 U.S. 322, 329–31 (1979). Relevant here is non-mutual collateral estoppel, which prevents the losing party from relitigating an issue against a *different* party. *Id*. Thus, non-mutual defensive collateral estoppel "precludes a plaintiff from relitigating identical issues by merely switching adversaries." *Parklane*, 439 U.S. at 326; *see also Lipin v. Hunt*, No.

14cv1081, 2015 WL 1344406, at *5 (S.D.N.Y. 2015). Courts are "generally accorded 'broad discretion' in determining whether or not collateral estoppel should apply in a given case." *Bear, Stearns & Co., Bear, Stearns Sec. Corp. v. 1109580 Ontario, Inc.*, 409 F.3d 87, 91–92 (2d Cir. 2005) (quoting *Parklane*, 439 U.S. at 331).

In *Muzin*, the same Plaintiffs as here brought RICO Act claims against purported foreign agents of Qatar, alleging that they partook in a "Qatari Enterprise" that conspired against Plaintiffs to hack their computers and disseminate the hacked information to the media. *See* 2020 WL 1536350 at *1. The "Qatari Enterprise" at issue in *Muzin* expressly included Qatar and its government and agents, Nicolas Muzin, Gregory Howard, Jamal Benomar, *Kevin Chalker*, Stonington Strategies LLC, *Global Risk Advisors LLC* "*and numerous known and unknown agents, including cyber hackers, public relations professionals, lobbyists, political actors, and others*." *Compare Muzin* Amended Complaint ¶ 199, No. 19-cv-0159 (emphasis added) *with* SAC ¶ 291 ("The Enterprise consists of, at least, *GRA*, *Chalker*, Mandich, Garcia, Courtney Chalker, GRA EMEA, GRA Maven, GRA Quantum, GRA Research, Qrypt, Bernoulli, Toccum, *Howard*, *Muzin* . . . *and numerous others known and unknown individuals, including cyber hackers, public relations professionals, lobbyists, political actors, and other members of the Qatari government*.").

The "Qatari Enterprise" in *Muzin* is unquestionably the same Qatari Enterprise that Plaintiffs allege violated the RICO Act in the present case. *See e.g.*, *Muzin* Amended Complaint ¶ 79 ("[S]ometime prior to December 27, 2017, the Qatari Enterprise retained Global Risk Advisors ("GRA") . . . to coordinate an offensive cyber and information operation against Plaintiffs, including by infiltrating Plaintiffs' computer networks and obtaining unauthorized access to Google email accounts"); *Muzin* Amended Complaint Section IV ¶¶ 78–110 (detailing the same exact alleged phishing scheme executed by the Qatari Enterprise as Plaintiffs allege in this case).

In *Muzin*, the court concluded that Plaintiffs—the same plaintiffs in this case—"failed to plead a pattern of racketeering activity because [they did] not plead either an open- or a closed-ended scheme." *See* 2020 WL 1536350 at *9. As a result, the *Muzin* court dismissed Plaintiffs' RICO claim and RICO conspiracy claim.[9]

Plaintiffs do not dispute that their RICO and Conspiracy to Violate RICO claims in *Muzin* were "actually litigated and decided." *Austin*, 270 F. App'x at 53. Nor do they contend that they did not have "a full and fair opportunity to litigate the issue." *Id*. Moreover, it is undisputed that the *Muzin* court's finding that Plaintiffs failed to plead a pattern of racketeering under the RICO Act "was necessary to support a valid and final judgment" to dismiss such claims on their merits. *Id*. Instead, Plaintiffs' sole argument against the applicability of collateral estoppel is that the issue in the *Muzin* proceeding purportedly is "not identical" to the issue here. Opp. at 13. Specifically, Plaintiffs argue that the issue is not identical because the Complaint here "was filed well after the complaint in *Muzin* and contains numerous allegations concerning these Defendants, which the *Muzin* court had no opportunity to review, let alone decide." Opp. at 13.

The Court disagrees. The *Muzin* court found that Plaintiffs failed to allege the required "pattern of racketeering activity" in connection with the *same alleged "Qatari Enterprise,"* pursuant to the *same exact statutes* that Plaintiffs now attempt to assert against parties that Plaintiffs had *identified as Muzin's co-conspirators* in the *Muzin* proceeding. The RICO Enterprise, the RICO claims, the elements of those claims, the alleged scheme, and the co-conspirators here are "identical" to those in the *Muzin* proceeding. The only difference is that

[9] In *Muzin*, after providing a comprehensive analysis regarding Plaintiffs' failure to plead "a pattern of racketeering activity" under the RICO Act, the court similarly dismissed the RICO conspiracy claim, "because an agreement to commit acts that do not form a pattern of racketeering activity is not an unlawful agreement under the RICO statute." *See* 2020 WL 1536350 at *11. Thus, the district court dismissed both RICO claims pursuant to the same legal theory and rationale—*i.e.*, Plaintiffs failed to plead "a pattern of racketeering" required for either to survive.

Plaintiffs now bring the claims against different alleged members of the same conspiracy. The doctrine of collateral estoppel " 'precludes [Plaintiffs] from relitigating identical issues by merely switching adversaries.' " *Lipin v. Hunt*, No. 14cv1081, 2015 WL 1344406, at *5 (S.D.N.Y. 2015) (quoting *Parklane*, 439 U.S. at 326). Therefore, the Court finds that Plaintiffs' RICO Act Claim (IX) and Conspiracy to Violate RICO Act Claim (X) are dismissed pursuant to the collateral estoppel doctrine in their entirety.

E. California State Law Claims

Defendants argue that Plaintiffs state law and common law claims should be rejected because each is categorically preempted by the CUTSA claim. CUTSA specifically provides that it "does not affect . . . civil remedies that are not based upon misappropriation of a trade secret." Cal. Civ. Code § 3426.7(b). Nevertheless, this provision has been read to "implicitly preempt[] alternative civil remedies [that are] based on trade secret misappropriation." *K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc.*, 171 Cal. App. 4th 939, 954, 90 Cal. Rptr. 3d 247, 258 (Ct. App. 2009). The "determination of whether a claim is based on trade secret misappropriation is largely factual." *Id*. "At the pleadings stage, the [preemption] analysis asks whether, stripped of facts supporting trade secret misappropriation, the remaining factual allegations can be reassembled to independently support other causes of action." *Waymo, LLC v. Uber Techs., Inc.*, 256 F. Supp. 3d 1059, 1062 (N.D. Cal. 2017).

Plaintiffs' remaining state-law claims alleging (1) receipt and possession of stolen property, (2) intrusion upon seclusion, and (3) civil conspiracy "each have a basis independent of any misappropriation of a trade secret." *Angelica Textile Servs., Inc. v. Park*, 220 Cal. App. 4th 495, 506, 163 Cal. Rptr. 3d 192, 202 (2013), *as modified* (Oct. 29, 2013). This is because those claims "do[] not require that the confidential information qualify as a 'trade secret' " in order for Plaintiffs

to prevail. *Integral Dev. Corp. v. Tolat*, 675 F. App'x 700, 704 (9th Cir. 2017). In other words, CUTSA "does not displace [] claims that, *although related* to a trade secret misappropriation, are independent and based on facts distinct from the facts that support the misappropriation claim." *Angelica*, 220 Cal. App. 4th at 506 (emphasis added). This is especially so here given that the Court has dismissed Plaintiffs' claims under CUTSA and DTSA after concluding that Plaintiffs failed to adequately plead Defendants possessed any trade secrets to misappropriate. As such, the Court concludes that CUTSA does not preempt Plaintiffs' remaining state-law claims.

i. Receipt and Possession of Stolen Property in Violation of California Penal Code § 496

Plaintiffs assert civil claims predicated on alleged violations of California Penal Code Section 496 (Count IV) against all Defendants. SAC ¶¶ 220–28 (Count IV). California law makes it unlawful for any person to "receive[] any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained." Cal. Pen. Code § 496(a). "Any person who has been injured by a violation of [this law] may bring an action for three times the amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney's fees." *Id*. § 496(c). At the pleadings stage, Plaintiffs must plausibly allege "three elements: (a) the property was stolen, and (b) the defendant was in possession of it, (c) knowing it was stolen." *Verdugo-Gonzalez v. Holder*, 581 F.3d 1059, 1061 (9th Cir. 2009); *see also Switzer v. Wood*, 247 Cal. Rptr. 3d 114, 121 (Ct. App. 2019). Plaintiffs adequately plead all three elements.

First, the SAC alleges that the information and documents stored on Plaintiffs' computer systems qualifies as property. This type of electronically stored information is "property" under California law, which provides that "[a]nything that can be the subject of theft can also be property under section 496." *People v. Gopal*, 171 Cal. App. 3d 524, 217 Cal. Rptr. 487, 497 (Ct. App.

1985); *see Am. Shooting Ctr., Inc. v. Secfor Int'l*, No. 13cv1847 BTM(JMA), 2016 WL 1182745, *5, *25, *26 (S.D. Cal. 2016) (denying defendants' motion to dismiss Section 496 claim, holding that "documents on the computer may . . . be deemed property subject to theft"). As such, the electronic information contained on Plaintiffs' computer systems constitutes property which is capable of being stolen.

Plaintiffs also sufficiently allege that such information was knowingly stolen and possessed by Defendants. *See e.g.*, SAC ¶ 111 ("From January 16 to February 25, 2018, BCM's server was subjected to approximately 325,000 malicious connections from 59 unique internet protocol ("IP") addresses."); SAC ¶ 116 ("Chalker told GRA personnel that Chalker and GRA were responsible for the hack-and-smear operation targeting Broidy/BCM."); SAC ¶ 117 ("Chalker also told GRA personnel that Chalker, Garcia, and Courtney Chalker had destroyed electronic devices and other materials containing evidence of the Broidy/BCM hacking"); SAC ¶ 232 ("GRA and Chalker . . . view[ed] [Plaintiffs' secluded documents and private communications] through electronic means and then print[ed] them out."); SAC ¶ 128 ("Defendants carefully packaged the hacked materials into a series of PDFs[.]"). Such specific allegations, accepted at true at this juncture, are sufficient to state a claim.[10] Defendants' motion to dismiss this claim (Claim IV) is denied.

ii. Intrusion Upon Seclusion

Plaintiff asserts a claim (Count V) against Chalker and GRA for intrusion upon seclusion. SAC ¶¶ 229–37 (Count V). Under California law, the common law tort of intrusion upon seclusion "has two elements: (1) intrusion into a private place, conversation or matter, (2) in a manner highly

[10] The Court notes that the SAC does not contain any specific allegations that Denis Mandich possessed the stolen information, except that one may draw an inference that as "the mastermind behind the Global Leaks operation, overseeing the execution of . . . the operation," Mandich necessarily would have possessed the hacked information at some point. *See* SAC ¶ 60. Nevertheless, as later discussed, Plaintiffs plausibly allege that Defendants, including Mandich, were a part of the conspiracy, which among other things, conspired to intrude on Plaintiffs' seclusion. Therefore, the Court does not dismiss this claim against Mandich at this stage.

offensive to a reasonable person." *Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 74 Cal. Rptr. 2d 843, 955 P.2d 469, 478 (Cal. 1998) (citing *Miller v. Nat'l Broad. Co.*, 187 Cal. App. 3d 1463, 232 Cal. Rptr. 668 (Ct. App. 1986)). For the first element, "the plaintiff must show the defendant penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff." *Id*. The defendant may be held liable "only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source." *Id*. For the second element, "each case must be taken on its facts." *Id*.

Defendants point to two cases that they believe show there is no reasonable expectation of privacy in emails. First, in *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1052 (N.D. Cal. 2018), the district court held that internet-based communications are not "*confidential*" within the meaning of Section 632 of California's Invasion of Privacy Act because such communications can easily be shared. *Id*. (internal quotations omitted). A claim for Intrusion upon Seclusion, however, does not require that the information at issue be "confidential," "only [that] plaintiff had an objectively reasonable expectation of seclusion or solitude in the . . . data source." *Shulman*, 18 Cal. 4th at 232. In *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1042 (N.D. Cal. 2014), the district court held that plaintiffs failed to allege sufficient facts to establish a reasonable expectation of privacy in emails generally based on the "mere fact" that defendants intercepted and distributed their emails. The court noted that it did not find "any case in the California or federal courts holding that individuals have a legally protected privacy interest or reasonable expectation of privacy in emails *generally*." *Id*. (emphasis in original). However, the court went on to state that "the cases in which courts *have* found a protected privacy interest in the context of email communications have done so in circumstances where the plaintiff alleged with specificity the material in the content of the email." *Id*. (citing *Mintz v. Mark Bartelstein & Associates Inc.*, 906

F. Supp. 2d 1017, 1033–34 (C.D. Cal. 2012) (finding legally protected privacy interest in the personal financial and employment information contained in an email account)).

Here, Plaintiffs do not solely allege that Defendants intruded upon emails *generally*. Instead, Plaintiffs specifically allege that during the hacking scheme, Defendants intruded upon numerous otherwise private or sensitive email communications and documents, including "signed contracts, attorney-client privileged communications and documents, attorney-client work product, usernames, and passwords to access other non-Google accounts, . . . financial information, and confidential business process and methods information." *See* SAC ¶ 117. Furthermore, the SAC alleges in detail that these materials were specifically hacked and curated in an effort to tarnish Plaintiffs' reputations. SAC ¶¶ 128, 132, 144, 148–50, 157–58.

Accordingly, this Court agrees with the *Muzin* decision, 2020 WL 1536350, at *19, and other decisions concluding that "hacking into a person's private computer . . . would represent an intentional intrusion on the victim's private affairs and that such an intrusion would be highly offensive to a reasonable person." *Coal. for an Airline Passengers' Bill of Rights v. Delta Airlines, Inc.*, 693 F. Supp. 2d 667, 675 (S.D. Tex. 2010); *see also Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1058 (N.D. Cal. 2014) (finding plaintiffs pled intrusion upon seclusion because defendants' copying plaintiffs' personal contact information and mobile address books was "highly offense"). The Court therefore finds that Plaintiffs have adequately pled their Intrusion Upon Seclusion claim (Count V). Defendants' motion to dismiss is denied with respect to that claim.

iii. Civil Conspiracy

Plaintiffs allege a claim for civil conspiracy against all Defendants (Count VI). SAC ¶¶ 238–46. Civil conspiracy "is not a cause of action, but a legal doctrine that imposes liability on persons who, although not actually committing a tort themselves, share with the immediate

tortfeasors a common plan or design in its perpetration." *Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal. 4th 503, 28 Cal. Rptr. 2d 475, 869 P.2d 454, 457 (1994) (*en banc*). In other words, when a co-conspirator participates in a civil conspiracy, that conspirator "incurs tort liability co-equal with the immediate tortfeasors." *Id*. To plead a civil conspiracy under California law, a plaintiff must allege: "(1) formation and operation of the conspiracy and (2) damage resulting to plaintiff (3) from a wrongful act done in furtherance of the common design." *Rusheen v. Cohen*, 37 Cal.4th 1048, 39 Cal. Rptr. 3d 516, 128 P.3d 713, 722 (Cal. 2006).

Defendants first argue that the Civil Conspiracy claim should be dismissed because Plaintiffs fail to plead an underlying tort. This argument is moot as the Court has already determined that Plaintiffs have adequately pled various underlying claims. Defendants further argue that Plaintiffs fail to specifically allege acts taken in furtherance of the conspiracy. The Court disagrees. The complaint alleges Chalker told GRA personnel that he and GRA were responsible for the hacking operation targeting Broidy and BCM. SAC ¶ 116. Chalker allegedly also "told GRA personnel that he, Garcia, and Courtney Chalker had destroyed electronic devices and other materials containing evidence of the Broidy and BCM hacking . . . to conceal the role of GRA and himself in the hacking." SAC ¶ 117. Mandich allegedly "furthered the illegal activities by . . . designing and strategizing the 'special projects' including covert operations at Chalker's direction." SAC ¶ 242. These all constitute specific acts taken in furtherance of the alleged conspiracy. As such, the Court finds that Plaintiffs have adequately pled Civil Conspiracy (VI) and deny Defendant's motion to dismiss the claim.

CONCLUSION

For the foregoing reasons, the Court resolves Defendants' motion to dismiss as follows:

- The motion is GRANTED with respect to all claims against Courtney Chalker on personal jurisdiction grounds.
- The motion is GRANTED with respect to all claims against the foreign Corporate Defendants on personal jurisdiction grounds.
- The motion is DENIED with respect to the Stored Communications Act claim against Chalker and GRA (Count I).
- The motion is DENIED with respect to the Computer Fraud and Abuse Act claim against Chalker, GRA, Mandich, and Garcia (Count II) and the California Comprehensive Computer Data Access & Fraud Act claim against Chalker and GRA (Count III).
- The motion is GRANTED with respect to the Defend Trade Secrets Act and California Uniform Trade Secrets Act claims in their entirety (Counts VII and VIII).
- The motion is GRANTED pursuant to the collateral estoppel doctrine with respect to the RICO Act and Conspiracy to Violate RICO claims in their entirety (Counts XI and X).
- The motion is DENIED with respect to Plaintiffs' Receipt and Possession of Stolen Property claim against Chalker, GRA, Mandich, and Garcia (Count IV).
- The motion is DENIED with respect to Plaintiffs' common law Intrusion Upon Seclusion claim against Chalker and GRA (Count V).
- The motion is DENIED with respect to Plaintiffs' common law Civil Conspiracy claim against Chalker, GRA, Mandich, and Garcia (Count VI).

The Court of Clerk is respectfully requested to terminate Docket Entry 123.

SO ORDERED.

Dated: New York, New York
September 26, 2023

Mary Kay Vyskocil

MARY KAY VYSKOCIL
United States District Judge